Privacy and Security Standards Workgroup
Draft Transcript
March 9, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good afternoon, everybody, and welcome to the Privacy and Security Standards Workgroup call. This is a Federal Advisory call, so there will be opportunity at the end of the meeting for the public to make comment. Just a reminder for workgroup members to please identify yourselves when speaking.

Let me do a quick roll call. Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Walter Suarez?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Jeff Whiteside, Blue Cross Blue Shield?

Jeff Whiteside – Blue Cross Blue Shield
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Steve Findlay? David McCallie? Wes Rishel? Sharon Terry? Steve Ondra? Mike Davis? John Moehrke?

John Moehrke – Interoperability & Security, GE – Principal Engineer
I am here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Ed Larsen? Kevin Stein? John Blair?

John Blair – Tacanic IPA – President & CEO
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
With that, I'll turn it over to Dixie.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay, I have a feeling people will be dialing in for a minute. We wanted to go over two things today. One is I want to start out by thanking those of you who have provided me comments on the digital certificate standards. As you know, it's gone through several iterations with really valuable feedback from multiple places, and I really, really do appreciate that.

We may as well go ahead. The topics on our agenda, first, we're going to go over these slides about digital certificates. Then, it's an hour and a half meeting and hopefully we'll get started on our discussion of the requirements for standards for provider directories. I wanted to remind everybody that the process

for developing standards is changing and this workgroup is at the front of the change. I know it's not always clear what we're doing here, but I wanted to make sure that everybody understands the new process as we understand it right now. Up until now we have really recommended standards, and now that the ONC has launched their standards and interoperability framework effort, we're changing into a more measured and less frantic, quite frankly, process to develop standards.

Whereby, in the past the Standards Committee has really recommended the standards themselves, we still will recommend the standards but we won't do the heavy lifting as much as we have in the past. The new model is that the Standards Committee will recommend requirements that the standard that is selected must meet. So we don't really select the standard right off the bat, we specify the requirements that the standard must meet and we specify the criteria that we will be using when a standard has been presented back to us. So we recommend the requirements for the standard, that recommendation goes to the ONC, who will give it to the S&I framework, and the S&I framework people will do the heavy lifting, so to speak, and come back to us with a recommended standard. Then we will use the evaluation criteria that we specify at the beginning to evaluate the standard to determine whether it meets the requirements that we gave them to begin with. So that's the new model that we're working within.

Let me go to the next slide. The last time when we walked through these digital certificate slides there was some confusion about where we were in the scheme of things. The first two slides in this deck are intended to be our recommended requirements and our recommended evaluation criteria, which is what I just described. At our first discussion and our last working group meeting we decided that there were a couple of questions that are really policy questions that we wanted to have the Standards Committee hand over to the Policy Committee to have addressed. The rest of the slides are intended to lay the groundwork of baseline understanding of digital certificates to set it up to ask the Policy Committee to address these questions. So I've inserted a couple of title slides here so that it's clearer when we make the transition into the second topic.

First, let's look at the two slides. One slide recommends standards and the other slide recommends evaluation criteria for a digital certificate standard. Again, this is for a digital certificate standard to be used for direct exchanges and I guess they're calling it NW-HIN standards.

Is that right, Judy, are they calling it NW-HIN standards?

Judy Sparrow – Office of the National Coordinator – Executive Director
I think they're calling it NW-HIN, yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what I—

Judy Sparrow – Office of the National Coordinator – Executive Director
Let's be consistent.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, for a while. I got some really good feedback, one thanks to Kevin Klein at NIST who put me in contract with David Cooper, who is one of the authors of 5280, which was most, most helpful. This is the recommended requirements as I currently perceive them based on what I've heard from the previous working group discussion and what I've heard since then. So let's discuss what I have here.

The X.509 Version 3 certificate profile is as defined in RFC 5280, which is the most recent update to the digital certificate standard. I think before we had the certificates must include the basic certificate fields that are defined in the RFC. Then in addition to those certificate fields the standard defines a number of extensions and from everything I gather from multiple sources, those that I have listed there are the ones that are most essential to have. The first one identifies where you get the public key that will allow you to read the digital signature for the certificate itself. The subject key identifier is—I think I have all these if you have what I sent out a while ago, you can look at the notes at the bottom and all these definitions are down there, basically what they do. Then we decided at our last meeting that these certificates must

support the authentication of the endpoints for both direct exchanges and NW-HIN exchanges, and that the certificates may include additional extensions, so we aren't precluding including additional extensions. We also discussed the certificate revocation list, their need to conform to the standard.

Is there any further discussion or—?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Dixie, are we saying that they must have all of these extensions or if the extension is valid for the use case, that these extensions be used rather than the creation of alternative attributes?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We only have two use cases, NHIN Direct and NW-HIN, so we're saying that these are needed in order to allow certificates to be used for exchanges on both.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well subject to alternative name would not always be needed.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I thought that that would always be needed for, now I might be wrong, but I thought it would always have to be needed because of the direct exchanges because they're over e-mail.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right, but it would not be needed for the exchange model. So that's why I'm saying there are some differences in how important these are based on whether you are using exchange use cases or direct use cases.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, and that's a question that I had that I would love to hear some discussion around. Are we asking them to come up with one standard that can be used on both, or to come up with two standards? It seems like the easy way would be to come up with two standards, but then you want everybody to be able to talk to everybody else.

John Moehrke – Interoperability & Security, GE – Principal Engineer
They're not mutually exclusive standards, by the way. It's just that I can have a certificate that is used only for direct communications and therefore it doesn't need some attributes, or I could have a certificate that is only used for session oriented and doesn't need the S/MIME attributes, but that does not mean that I can't have a certificate that's used for both purposes. So they're not mutually exclusive. It's just as soon as we say that the certificate must include all of the following standard extensions, and I just didn't see the word "all" so I wasn't as sure of how we meant that—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I meant it as all, but I didn't get if what you're addressing is critical or not.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And I didn't really include the critical, but the subject alternative name could be non-critical, in which case it wouldn't need to be processed by NW-HIN.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right, and extended T usage would be unnecessary for—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
You're exactly right.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I don't have a problem with saying now if the use case needs the attribute these are the ways to communicate the attribute. So I don't even think that's controversial. But to say that all certificates have to include all of these attributes may not be the right way to go about it.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
It seems to me that there is a—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The way it works is it looks at the extension and the standard handles that through the use of these criticals and non-criticals. So you could have all the attributes there, but if it said it's non-critical then it would not need to be processed.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
The question to me is whether these extension attributes are not so much critical in my mind, but applicable even to—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what that means.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
So my suggestion is really you can include in the second bullet that certificates must include the following standards as applicable, and then clarify in a couple of them, for example, subject key identifier applicable to direct exchanges, something that clarifies that these standard extensions are only required when applicable to the specific use case that is being applied to.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
One thing I've learned from talking to David Cooper, who's the author of 5280, is that the way "critical" is used in that standard doesn't mean it's a critical field. The word "critical" means that if that field is there it must be processed. The way you would handle applicable would be to make it a non-critical field. So it would also need a certificate, but it would not always have to be processed.

John Moehrke – Interoperability & Security, GE – Principal Engineer
In that particular direction I agree, the standard handles it quite well. The direction I'm coming at from, though, is the opposite, and that is, if a certificate authority is only issuing certificates for the NW-HIN Exchange and therefore knows it will never be issuing certificates for use with the Direct Project, this would force them to put in the attribute and mark it as non-critical .... I just was wondering if that's our intention, that the current certificate issuing system, which I don't believe puts all those in there, is now non-compliant, even though they're non-critical attributes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, so you're saying take—the problem I have with "as applicable" is that a machine doesn't understand as applicable. So I would be much more comfortable separating those two attributes out and saying certificates used for direct exchanges must include these too, or taking them out entirely. I'd be okay with that. But I don't think a technical spec should say "as applicable" because—

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I wasn't meaning that this would be—I don't know that this reads as a technical spec more than as a policy treatment.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that's true. It's a requirement ..., that's right.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I don't think we're far off. I just think—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What would you suggest? Do you want me to take those two out?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Dixie, first, just to let you know that I joined a little bit late and second, aren't we just talking about two profiles—one for Direct and for NW-HIN?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what I was just asking. I think yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
And just specify the profile as part of the—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think we ought to say that you need to specify two certificate profiles to elevate that certificate to must support and say that we want two profiles.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Because I was just sitting here reading the RFC while you guys were talking and there's a fair amount of optionality in there, even as well written as it is, so a profile—

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
—... clarify exactly how to do it for those two use cases.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, and the optionality ... because of these kinds of different uses, so I was concerned we were getting overly restrictive on the optionality that already exists.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I agree with David, we need a—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The standard shouldn't have a whole lot of optionality because people will find themselves, I've got a direct connection and I can't talk to anybody because at the other end they're expecting certain extensions that aren't there. So we need to be prescriptive enough that the exchanges can occur.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, but these are not the usual attributes that cause communications to fail.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Anything that a machine expects and is not there or doesn't expect and is causes it to fail.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think we're in violent agreement here. We're saying that the use cases might be slightly different and we handle that with the profile. I'm using profile in quotes. I don't necessarily mean a formal standards body profile.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, it seems to me in this policy statement what we can do is clearly the first rule of certificate must include, we can add a statement about "Certificate for Both Direct and NW-HIN Must Include." Then a second bullet, "Certificates for Direct Purposes Must Include the Following Extensions." Then a third one, "Certificates for NW-HIN Purposes Must Include the Following Extensions," and then add the ones. Then I think that will probably help create the guardrails for the application of this certificate profile.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
If we did that then the second bullet you would take subject alternative's name and extended key usage out and put those on the Direct one only.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I don't think we need to necessarily mandate any of those extensions.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What would you put?

John Moehrke – Interoperability & Security, GE – Principal Engineer
I would just say that if the attributes are necessary they must be communicated in the way defined by 5280.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
How about if we have the first one is, "All Certificates Must Include the Basic Certificate Fields," and in the second bullet we pull up this down here at the bottom, "Certificates for Direct Exchanges Must Include Extensions Appropriate for Secure E-Mail." Then, "Certificates for NW-HIN Exchanges Must Include Extensions Appropriate for COS Connections." Is that what you want to say?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Not really, because then that leads the question to, what are those extensions?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that's—

John Moehrke – Interoperability & Security, GE – Principal Engineer
My answer is the minimal extensions are in the basic fields.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, they aren't.

John Moehrke – Interoperability & Security, GE – Principal Engineer
The minimal extensions are not critical.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, they aren't. That's not true. That's one of the things I learned from David Cooper. The minimal are not necessarily in the basic fields. There are some extensions that are essential. Those that he mentioned to me are Authority T, Subject T, T Usage, and Certificate Policies.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
John, are you saying that if we say certificate for direct must include, for example, Authority T identifier, that's not always the case?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It is always the case.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I'm just asking John if he thinks it's not.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I'm not sure about those, and when Dixie reads through those four I don't have a direct problem with those. Those are not the concern I'm worried about. It's the ones following that. But I would rather us not get too wrapped around it. If 5280 says these are the basic fields and these are the extensions, what evidence are we using to override their optionality?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
There have been a number of profiles published by various organizations and apparently they're well known which fields are always needed. Those four are always needed, even though they're extensions. I'm here to do what this team wants to do, but my concern is that we have to put requirements at sufficient levels that we're able to say, yes, this standard meets our requirements, or no, it doesn't, only ambiguously.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
It seems to me that when you put the sub-bullet numbers, 1, 2 and 4, jumping over 3 for a minute, we're saying there is a minimum, that basic field that must always be included. And then on the other end we say, on the fourth sub-bullet, "Certificate May Include Additional Standard Extensions." What we're doing with the second sub-bullet is creating additional minimum must-includes for specific applications. John, you don't seem to be comfortable with bringing from the standard extensions some that "must be" rather than that "may be."

John Moehrke – Interoperability & Security, GE – Principal Engineer
And that's just because I have not experienced evidence that says that those have to be mandated, that's all. I don't recall us talking about evidence on the last call. All of a sudden they went from being "may," which is the fourth bullet there, to "must" and I went whoa, wait a minute, why did these go to "must"?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
"Must" means it must have the extensions required for NW-HIN and Direct. That's what we used to say. Maybe that's what we need to go back to. It always had one that said "it must include the extensions needed for these two exchanges on Direct and NW-HIN," and then we had "it may include additional." So maybe that's what we really need to say.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Could you say that one more time, Dixie?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It originally said that certificates must include the extensions required for, and then one sub-bullet was Direct Exchanges and the other one was NW-HIN Exchanges as defined in 5280. Whereas, now it just says authentication of endpoints. It would basically say, the third bullet would read, "Certificates Must Include Standard Extensions as Defined in Section 4.2 of RFC 5280 for...," and then the first sub-bullet would be Direct Exchanges and the second would be NW-HIN Exchanges.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
And not detail those that are on the second sub-bullet.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, I think that would be better.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, I like that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think that would be better because there's another problem with the third bullet, is that it only addresses the authentication and Direct does more than that.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Let me change it like that and I'll send that out to you. I'll give you guys a break and I'll just send that, if you want. Well, let's see how far we get.

These haven't changed much at all except to update it to 5280. The second bullet is how the requirement would more or less read, "Certificates to be Used in Direct Exchanges Must Include All Basic Certificate Fields and Those Extensions Required for Direct Exchanges." Does that make sense?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. I think that is better.

John Moehrke – Interoperability & Security, GE – Principal Engineer
The question that does come up is this is very CRL based, as opposed to OCSP.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, you know, 5280 includes OCSP, not just CRL. In fact, the CRL extensions include OCSP field values, so this doesn't exclude OCSP at all.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well, it's not stated and as read it could very easily be read that CRLs must be not only published but CRLs must be the mechanism to use for revocation checking.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, that's not true, John.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I don't have a problem with CRLs, I really don't. The question is some prefer to use OCSP.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It doesn't. Because I started to put something in there about OCSP because you brought it up the last time, but whether you pull down the entire CRL or OCSP, those are the protocols used to check the CRL, not the standard used to represent the revoked certificates. So if you look at the standard, the list of revoked certificates can be ... using either the OCSP protocol or pulling down the whole CRL. In fact, there's a line in the standard itself that says either one can be used. I started to put it in there but that seemed to me like a policy rather than a standard since the standard supports both.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Okay. I agree with your technical assessment, I'm just saying the way that the presentation reads to someone who does not know that, they may not realize that CRL in this context is talking about the greater concept of a certificate revocation list and not the specific file format, which is a CRL file format. I'm just wondering if there's a word we can introduce.

M
Dixie, I agree with John too. I had the same question.

John Moehrke – Interoperability & Security, GE – Principal Engineer
If there's a word we can introduce or something like that, that's all we need to do. We don't need to actually even include the OCSP, but we need to make sure that it's clear that the task of checking for certificate revocation is important but it's not necessarily the file format.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think all we need to do is on the requirement on this slide, on this last one we can just add "which supports both OCSP and full CRL."

John Moehrke – Interoperability & Security, GE – Principal Engineer
Good.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And just make it real clear.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, that's important. I neglected to include in the glossary of terms OCSP, and so to John's point, we don't mention it in here, we don't mention it in any other place, so it might give the impression that we're only talking about CRLs. So I think in addition to including it in this slide, we'll make sure to include it in the glossary as well, just to reference it there.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. So the requirement itself won't change, it will just clarify that it supports OCSP, yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I have a question from a naïve point of view. Does the allowance of either of these two approaches to certificate revocation decrease the interoperability? In other words, is there an advantage to selecting one and just saying for the particular use cases this is how it should be done to facilitate interoperability, or is that not necessary?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Actually, my experience is when you try to constrain this particular piece you actually decrease your interoperability. Most implementations of code that checks certificates for whether they're valid, whether they're being used within the policy use and all that, have built into them both CRL and OCSP checking and certificate authorities can usually support either/or. It usually comes down to a question of what is the easiest to access. Is it easier to access an online transaction that must succeed, and we know how to handle failing OCSP, or is this particular instance a remote system that will pull down a CRL every 24 or 48 hours and deal with it off line. It then becomes very much an implementation detail. You basically just simply say you have to support both, and that's not a difficult task from a technology perspective.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's not even a difference in field values or extensions or anything like that.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Correct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's just how you access the information. In fact, I'm looking at 5280 right now, and here it says, "Revocation status information may be provided using the online certificate status protocol, OCSP, certificate revocation lists, or some other mechanism." So it allows for whatever, it's just an implementation detail.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's good and that's helpful. That raises another question that's just on the edge of things from a policy point of view that John's use case brought into my mind, is have we heard any discussion or do we feel any need to talk about the timeliness of the revocation, given the—

John Moehrke – Interoperability & Security, GE – Principal Engineer
Oh, please not us.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's another policy issue we need to toss back over the fence, David.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I know it's a policy question, but it might be something to identify.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, it's a policy question and it's one for which you will watch policy committees just spin forever on, because it is one of those where you say, well, gee, we don't want a revoked certificate to be used a picosecond after it's been revoked, but when you actually look at the practical realities of this, you start looking at it and saying well, 48 hours is really about the best we can make sure that everybody has been updated on. Yes, the NW-HIN Exchange spent a long time on that topic.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, there are a number of time windows specified in meaningful use, so it's not out of the question.

John Moehrke – Interoperability & Security, GE – Principal Engineer
No, but it's one of those that's a no win. To actually have the Policy Committee say yes, we're willing to let certificates be used for two, three days after it's been revoked is a very difficult thing for a Policy Committee to allow.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That would be a good meaningful use measure. We don't have any good ones.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, I agree. It is a value that needs to be brought up—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Mike Davis, I heard his name. I'm sorry. I didn't mean to— Mike Davis, I heard your name a while ago. In the federal PKI's assurance levels, do they address how often they have to be checked?

John Moehrke – Interoperability & Security, GE – Principal Engineer
I don't know if Mike's on today.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think I heard him.

Mike Davis – Veterans Health Administration – Senior Security Architect
I'm on. I'm on mute. I'm in a little office right now. No, those are policy issues that in my experience, as John said, have been argued over as to how many picoseconds or days ... out, so that's a common discussion.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Interesting. So I'm going to add the OCSP reference to the requirement slide. Are there any other comments about this slide? Okay, I will do those updates and get them out to you. Now, we go into the second part, and these next slides are intended to give the Policy Committee a real basic understanding of what digital certificates are and how they're used, and then all leading up to the questions that we ask them in the last slide. I got some good feedback from Anne Castro, and I'm trying to make it easy to

understand, so let's see. This is the background on what a digital certificate is. I don't think this has changed since the last time we saw this, right? Oh no, the last bullet I reworded slightly in response to one of Anne's comments that it was too hard to understand what it was saying. I hope that's clearer. But if any of you have any suggestions as to how to make this easier to understand, I sure would appreciate it.

John Moehrke – Interoperability & Security, GE – Principal Engineer
The one thing that I did note when I was reading this was, and I don't know if this is too technical, too in the weeds, but oftentimes people get confused by the fact that the revocation list only includes the certificates that are currently valid, i.e. they haven't expired but have been revoked. I don't know if that's too far into the weeds, but I know plenty of policy people kept looking at certificate revocation lists and thought they were an ever increasing list that would become huge. The answer is no, they're self-limiting by the validity dates of the certificates.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Which indirectly raises another question about specifying the validity period for certificates, I don't know if it's just one of these questions to toss back over there.

John Moehrke – Interoperability & Security, GE – Principal Engineer
By the way, I was thinking after we moved on, I think we should probably recommend that they don't set that validity date or the revocation window too small.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Is it better to say in the second big bullet there that at the end instead of "that no longer are valid," say "that have expired."

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That have expired, yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Because really valid could mean a lot of things to people.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, valid really in the certificate business means that it is not expired, but I would add the words.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
So you would change that to, "that have expired?"

John Moehrke – Interoperability & Security, GE – Principal Engineer
No, "those certificates that are no longer valid and have not expired," so be redundant.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I see, okay. I can't write it on your screen, but I'm writing it on my copy. Good. These are the two pictures I added. I think Joy and Deborah suggested we have a couple of pictures. Actually, creating these pictures was useful to me too in that I came to a much better understanding of how the Direct Project works. It's really not a web of trust in the sense of PGP type web of trust, it's really what Arien calls a "multi-root model," where an individual user trusts certificates that were issued by trust anchors, they call them, they're CAs that that user trusts. So there's not necessarily a cross-signing between them, it's just that they know that they trust this trust anchor and so they trust all of the certificates issued by that trust anchor, so that's how it works. I made the hierarchical PKI real, real simple.

John Moehrke – Interoperability & Security, GE – Principal Engineer

You may want to, just to be more politically friendly with your big circle, include the trust anchor on both of them. What you did is absolutely proper, but I have been unsuccessful at getting many people in the Direct Project to recognize directly trusting a certificate. They always want the Direct Project to trust an anchor.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I see. Can you see my pointer? You probably can't. The large egg on the right should include both anchors.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Correct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that's a good point. Yes, I will definitely fix that.

John Moehrke – Interoperability & Security, GE – Principal Engineer
The model you have, by the way, is one I tried to push, because it does work too. But essentially the model the Direct Project wants, for simplicity sake, to advertise is where you're always trusting anchors.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that's a good point. Thank you.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
There are two levels of anchors there on that side of the picture, the root CA and the CA. I'm trying to understand really, so trust anchor root CA in the middle is the root CA for several other CAs, right?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, there are only two levels here, but the trust anchor other than the root could be a CA for a bunch of other trust anchors. So those trust anchors can be pretty deeply embedded. It may be useful to add a third level as well so that we can make that point.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
But is there anything that connects their root CAs?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No.

John Moehrke – Interoperability & Security, GE – Principal Engineer
No, not in the right hand model. That would be the left hand model.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's the key point.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
That's the key difference between the hierarchical PKI and the—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Exactly.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Correct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Exactly right. By the way, this multi-root model is consistent with 5280. It talks about trust anchors and 5280 is very flexible. This is just to give them, I don't even know whether this is useful or not, but I'm really trying, I hope you can even tell, very hard to establish some basic understanding of what we're

talking about. These are some of the basic fields that are in a certificate. These are just some basic uses of certificates just so that here's how they're used, just to try to convey that. The only one I changed was this last one, because in truth I was trying to illustrate how it can be used for encryption. In general it's used really to encrypt the key that's used for encryption, but I didn't want to get too convoluted. Let me know, is that clear enough?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Some people might ask or wonder or they're confused whether there is a difference between digital certificates and digital signatures. So in this particular slide there might be an opportunity at the bottom or something like that to make a note about the difference between—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's this one really, to digitally sign, that's a digital certificate. Maybe I should put digital certificate in parentheses or something.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Digital signature, do you mean?

John Moehrke – Interoperability & Security, GE – Principal Engineer
But the signature is the result of the signing, right?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, it's a result of the signing, yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
That's what might be helpful to add, yes, maybe in that second sub-bullet.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what I have here. I say the sender signs the content using its private key, and that's what this is, the digital verifies the signature.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, I think what Walter's asking is on the previous page, that the digital certificate itself is signed by the CA that issued it. That first sentence just needs to be called out a little bit stronger.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
... it has the signature of the CA that issued the certificate.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. Walter, yes, a digital certificate is signed itself by the certificate authority that issued it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
And then it in turn can be used to sign other things, which is where it gets confusing.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Well, that's what it does. The second point, the one that David just mentioned, I know that the digital certificate itself has a digital signature by the certificate authority, that part I don't think is the one I was worried about confusion. The one that I'm worried about confusion is people thinking that a digital certificate equates to a digital signature on some document.

John Moehrke – Interoperability & Security, GE – Principal Engineer
The result of the second bullet to digitally sign is a digital signature.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Then that is what I was suggesting be included in here, the result of this digitally sign is a digital signature.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay, I see. I can do that. I'll just add a bullet that says the result of the digital signature.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay, good, because they probably have heard of that, yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Oh yes, the biggest confusion among a lot of people is equating the two and not separating them and realizing that one produces the other but they're different.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay, done. Now, this one, Anne Castro said that it was a scary slide, and it has a lot of words on it and when I went back over it, it seemed like all these words are pretty needed, but how can we make it simpler and less scary?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Can we raise it up a level and just say they're used for authentication purposes, for encryption purposes and for signature purposes?

John Moehrke – Interoperability & Security, GE – Principal Engineer
That's what the previous slide did.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's the previous slide. This one is setting the stage for our questions. The intent of this slide is to make them realize why you need assurance in your CA. That's really the intent. It's two questions; one has to do with how can you trust the CA and the certificates it generates; and the second question is, should these digital certificates be required to be cross-signed with the federal CA. So the point of this is to set up why we're concerned about whether any given CA should be trusted or not and their certificates. Then secondly, is why it might make sense to require that these CAs be cross-certified with the federal CAs.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Dixie, I don't think you can reduce it too much. The term in there that is new and that I stumbled on a good bit in the learning process here was this cross-certified. I wonder if you could resort to another drawing to show, take the other drawing and show what it would look like if the multi-roots were cross-certified—

John Moehrke – Interoperability & Security, GE – Principal Engineer
That actually gets more confusing.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
—... a dotted line or something.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We're not really asking whether all the trust anchors should be cross-certified, but whether those CAs that provide certificates for health need to be cross-certified with the federal bridge CA to allow people to exchange information with the VA and the CMS and the federal agencies. Does that make sense?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, it makes sense. I just was thinking, to illustrate the fact that you're cross-certifying an intermediate layer CA instead of to the root. That's a good point. Then you could illustrate that with just a dotted line, but then you've got to put a dollar sign by it and say how much it costs.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, then you have to—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So the answer is, sure, why not?

Mike Davis – Veterans Health Administration – Senior Security Architect
Actually, I had a discussion on this recently with some of the safe people and some of the vendors and I'm not so sure that the cost issue is valid. We probably need to have some people maybe come to the committee and talk to us about that. When I talked to Safe and the vendors I'm told that you can get certificates that are acceptable under iCam for $60 for a three year license. At $20 a year, that just doesn't strike me as an insurmountable burden and it eliminates a hell of a lot of confusion.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well, I think if we put it that way, it may be the better way to put it, as to say, we should investigate the mechanisms that could be used to simplify with prompt certification of the federal bridge, and open that as a topic for policy.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Actually, I don't think we'd need to do that, John. I think this workgroup could recommend that directly to the ONC, because that's really not a policy. That's information gathering to really ferret out what is involved in cross-certifying. Then we can go back to the Policy Committee with some real data that says here's what it costs. Now, what do you think?

Mike Davis – Veterans Health Administration – Senior Security Architect
I like that. I'm just chiming in. That's the heartburn I guess I had last time, but I couldn't express in our discussions is that we're presenting a Policy Committee with a lot of technical data and asking them to make a decision but the technical decisions should be based on facts and some research and stuff like that and some options to be presented to policy makers, not asking them to make the technical decisions.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I think a full slide just on that one topic, that says look, we think a lot of the certificate stuff could be simplified by ONC's looking at what it would take to issue certificates for both use cases off of a federal bridge cross-certified CA.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I love that suggestion.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I like that suggestion too.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Just one other point; I appreciate, Mike, your coming up with some numbers, the debate that raged when Direct was talking about this was not so much the dollar cost of the certificate but what process cost there might be to a ... that wanted to go through and qualify—

Mike Davis – Veterans Health Administration – Senior Security Architect
Right, and the costs cited included the registration cost. So if we're interested I might be able to arrange some testimony from people who are doing this.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that would be great.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, that would be great.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I think the point that David's trying to make, Mike, is that we know that certificates from existing cross-certified CAs have been made reasonable. The discussion that David's bringing up is what if a ..., and we'll bring out maybe a PHR vendor, wants to become a cross-certified CA.

Mike Davis – Veterans Health Administration – Senior Security Architect
Exactly, so there are specified policies that are available that say what you have to do to achieve that.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right, and that piece is very difficult and onerous, and it should be.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
And it should be because it's such, you know, machines in cages behind rooms with perimeter protection, etc., types and multi-key access, there's a lot of stuff there that might be seen by some people as inhibiting wide uptake. That was the debate we had.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But there are levels of cross-certification too. They have ten different policies, there's a whole document assigned to the policies and so you wouldn't have to be cross-certified at the highest level of assurance.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Which level would be necessary to participate?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think recommending that the ONC undertake that would be a really good thing to do.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

John Moehrke – Interoperability & Security, GE – Principal Engineer
... this slide and put it as a standalone slide making that assertion, I think that would simplify this slide quite a bit.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
One question about this slide is whether these statements, which are going back to the Policy Committee, are statements of a decision by us to recommend this, or as statements asking the Policy Committee to make these recommendations. In other words, the second bullet says certificates used by federal agencies, all must include the assurance level under which they were issued, and that's a statement of fact, but the next bullet says certificates used to exchange information with federal agencies must be issued a cross-certification, that seems to be a statement of fact as well.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Then the last two bullets seem to be statements of our recommended policies more than fact.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's a statement of—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That last is existing policy, right?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It is a statement of fact as well. The six, those are all statements of fact.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
... in there.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Pardon?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Number six is a "may."

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
May, right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
The decision is not up to. It's not a fact ....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That first question really is, should there be some minimum level of assurance of the CA that issues certificates?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
My question is really the purpose of this slide, besides educating the Policy Committee, is it to ask them to make a specific statement from the policy side about any of this?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, the purpose of this slide is to set them up to ask at least two questions. We need a policy around the CAs and the certificates they issue, how do they make sure that the certificates, you know, these levels of assurance. The second one has to do with the cross-certification of CA. I think what I'm hearing is we want to take this off of here and bring it back into the first part of the presentation as a recommendation to ONC to study what it would take to enable CAs to get cross-certified with the federal bridge CA, right? Is that what I'm hearing?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. From my perspective that would be—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I go back to this slide and I remove all the federal bullets on it, put them together as a background slide to a recommendation that would say something like, given that certificates used to exchange information for federal agencies must be issued by CAs cross-certified, what would be required for a CA in the private sector to be cross-certified with the federal bridge. Then we recommend that ONC undertake an information gathering effort to find this out. Is that what you're saying, specifically to cross-certify ... with the federal bridge CA?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
We could recommend that they go find out what the costs are, and we could also, I thought we were pushing one step further and just say take responsibility for it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I think that—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Maybe that's too much federalism or too much federal control for the current political era.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
If it's really a reasonable cost, that's the next logical question that would come up, is heck, we can just do this. But we can ask it explicitly too. It may be worth asking whether there are any legal barriers to the government just doing that. I'm sure there aren't. Money.

John Moehrke – Interoperability & Security, GE – Principal Engineer
There may be some legal issues.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We can ask that. Any legal—

John Moehrke – Interoperability & Security, GE – Principal Engineer
We don't have Adam on this call, which is too bad.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
—issues. Okay, I'll make those changes. Now, I broke this first one out a bit assuming this ... is going to go away. Do you agree with these bullets, sub-bullets? Somebody suggested I take Direct, it used to reference only Direct, because the CAs that issue certificates for the NW-HIN Exchange I think already have governance, right?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Well, that's the point. If you go one slide back, the bullet that is second to last gives that impression, that certificates used by NW-HIN gateways must link back to an approved root CA. An approved root CA, I assume, is a federal bridge cross-certified root CA.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Only if we succeed at having all certificates issued from a federal cross-certified bridge, yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
The question is, are all the certificates used in NW-HIN issued by cross-certified CAs with a federal bridge?

John Moehrke – Interoperability & Security, GE – Principal Engineer
No.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, but according to the documentation they're all issued by the same root CA.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Today the NHIN exchange, which I think using the word NW-HIN gateway is not necessarily synonymous with the full exchange, are all issued from one certificate authority.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Is that cross-certified, the federal bridge?

John Moehrke – Interoperability & Security, GE – Principal Engineer
No, because they haven't been able to get that kind of authorization. We're saying we should get that authorization.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Then one point about this slide and one point about the next one. In this slide, the second to last bullet gives the impression that because it comes right after the bullet that talks about certificate use to exchange information federal agencies must be cross-certified, and the next bullet says certificates used

by NW-HIN must link back to an approved root CA, gives the impression that we're linking an approved root CA to cross-certified and so I would probably clarify that bullet—

John Moehrke – Interoperability & Security, GE – Principal Engineer
What I was recommending before when we were talking about the cross-certified discussion is that fourth bullet on cross-certified I think we should move off of this slide as a standalone recommendation. That way we won't be confusing these concepts, which are truly just simply building trust concepts, with cross-certified.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
But, John, let me suggest one thing and see if this works. My sense is the first four bullets on this slide are statements of fact related to just general CA and cross-certification with the federal bridge. Those last two bullets are the ones that I would pull out of this slide and put it in a separate slide that are the ones related to the applicability of CA cross-certification to NW-HIN and to the Direct Project.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
John, I don't understand how the NHIN Exchange can possibly not be cross-certified with the federal bridge since federal agencies are part of it.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Because they're not actively communicating patient data yet. I don't know either.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But they are. The Beacon community in San Diego and elsewhere, Kaiser, VA, and the military health system are all exchanging health information among them. So I don't understand how they can possibly not be cross-certified with the federal gateway. Mike, are you still on the line? I think Mike knows the answer to that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This has always struck me as one of the options is that you can pull everybody up to the federal bridge level or you can carve out policy and it's just policy, it's not law, that allows the particular transactions to flow without federal bridge. You can just say anything that's at a certain level of assurance can flow.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right, which is what I understood they were doing.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think that's what Exchange is doing. So it doesn't mean it's a given that everybody has to be cross-certified. That's an option, but it may be an expensive option.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right, and that just goes back to slide number eight on multi-roots model.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right.

John Moehrke – Interoperability & Security, GE – Principal Engineer
That's why that slide is there is to show that you can have a multi-root model. You don't have to always bridge, but if you bridge it does make your life easier.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, it reduces some barriers but it comes at a cost and policy has to decide whether the gain in comfort of trust is worth the cost. I think when we throw consumers into this, the notion that $20 a year for a certificate for a provider isn't too expensive might apply, but $20 a year for a consumer of a PHR is totally out of the question.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I don't think you'd be talking about—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
No, but they're going to be participating in Direct, so their circle of trust might not overlap the—

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
But going back to that slide number eight, isn't NW-HIN Exchange a hierarchical PKI with a single root CA, at the end of the day since today now that is the case?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That is the case for Exchange today.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Except for this unknown, which is then how do they communicate with the VA?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, we need Mike on the line. I can follow up with Mike to understand that. That's what I'll do. I'll follow up with Mike Davis to understand that and pull that whole discussion out to a recommendation on looking at what it would take.

John Moehrke – Interoperability & Security, GE – Principal Engineer
The technology isn't difficult. Those are two different policy choices and there are even transitions between policies that can be done. So to say that it couldn't possibly be anything other than at this point in time I think is kind of—

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Then it goes back to slide 12, which is the question you originally had, Dixie, about number 2 on slide 12.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Do you guys still see the slide?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, we're on slide 11 on the screen. Let me see if I can move it to slide 12.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
My Adobe Connect got killed.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, I just moved it to slide 12 on the screen.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Nothing's on my screen except "Adobe Connect network connectivity was lost."

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
So you're disconnected, but I'm still connected and I still control this.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I can see your changes, Walter, so I—

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I just moved it to slide 12, Dixie, and the question on slide 12, number 2 was whether the last statement, should all CAs issuing certificates using direct exchanges be required to cross-certify. One question was whether we should just say used in both NW-HIN Exchange and Direct Exchanges be required to be cross-certified with the federal bridge. That's one question. The other one is, well, that question, is it should "all," or the other alternative is to do it multi—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But we decided that we would not ask the Policy Committee about number two for now and instead ask the ONC to undertake an effort to do some fact finding around what it would take for that to happen.

John Moehrke – Interoperability & Security, GE – Principal Engineer
All right, so we're changing it from a question to the Policy Committee into a statement to ONC that if they can make this happen, the certificate management would be a much easier task.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, and I said I would talk to Mike Davis to get the facts right that would back up that question. But as far as what we ask the Policy Committee it would just be question one.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, and by the way, I think we need to clean up question one as well.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay, good. How?

John Moehrke – Interoperability & Security, GE – Principal Engineer
I think that was where we were laughed at as well.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
To be what policy—

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
When we said that we need policy around CA they will wonder what do you mean by we need policy around—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what the sub-bullets are about. We need the policy about the level of, I think what we've talked about before is we need policy around how do you establish assurance in a certificate, as well as how do you establish assurance in a certificate authority. You'll recall that people didn't like us using the word assurance, so they changed it to reliability and other things. But that's really what we're asking, so how do we say that succinctly?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Is that what you meant by the first sub-bullet? I didn't get that.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I didn't get that either.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, I think—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I was trying to avoid—

John Moehrke – Interoperability & Security, GE – Principal Engineer
—... where you want to go, so I think we may want to also change this into a statement that we need policy around the certificate authorities. One is, they need to have a well-defined level of assurance of identities prior to issuing a certificate, so make them more statements rather than questions.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Excellent.

John Moehrke – Interoperability & Security, GE – Principal Engineer
One is the level of assurance—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It—

John Moehrke – Interoperability & Security, GE – Principal Engineer
—of an identity prior to issuing a certificate.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay, I put my phone down because the fax is finished, I think. So I now say we need policy around CAs and the certificates they issue. Then the first sub-bullet should say, and I'll just type it as you say it.

John Moehrke – Interoperability & Security, GE – Principal Engineer
"The level of assurance that must be achieved prior to issuing a digital certificate."

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I would add the word "defining" the level at the beginning. "Defining the level of assurance," so ... policy defines the level of assurance, right?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Is that level of assurance essentially identity proofing in this case?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Maybe we should be specific or put that in parentheses so they know—

John Moehrke – Interoperability & Security, GE – Principal Engineer
You should put that in parentheses, yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Exactly. I think that will help us to think about what this is about.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay, and then the second one should read what?

John Moehrke – Interoperability & Security, GE – Principal Engineer
I think if we—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is where the trustworthiness and reliable—

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, this is the mechanisms that certificate users would use—oh boy, how—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What this is saying is how do you know that a certificate issue isn't a fly by night operation.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
As a recipient of the certificate or as a recipient of a –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, ... your ... list of certificates.

John Moehrke – Interoperability & Security, GE – Principal Engineer
When evaluating a certificate authority, right, that's the stuff that you're—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

John Moehrke – Interoperability & Security, GE – Principal Engineer
That would be a—boy, what is that called?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I heard somebody talk about this one time, that it's sort of like the California restaurant rating mechanism, where if you see an A in the window you know it's a clean restaurant, that you would have some way for somebody who's buying a certificate to know that this is a good place to go to get it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Isn't that—they call it CPS or something, Certificate Policy Standards or something? CP and CPS are the two terms that vaguely I remember reading.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's in 5280. That's the certificate authority that they must do such and such. But this is beyond even that. The policies that they use—

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
In our grocery we have certificate policy and certificate policy statement.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's what I'm thinking of.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Those are the ones. We have it defined in our glossary, but I think you're talking about certificate status authority, a trusted entity that provides online verification of a subject certificate.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
A certificate, yes, you're talking about how do you know you can trust a certificate authority? How do you know they're legitimate?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
You use a certificate status authority.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
... not going to go out of business the next week.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, it's the mechanism you use before you provision them through the creative solution.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO

Isn't that something called a certificate status authority, an authority that certifies the status of a certificate authority?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

John Moehrke – Interoperability & Security, GE – Principal Engineer
That's one service offering is you can outsource. It would be like contracting with lawyers to do something. But I think what we're trying to get at is what's the general mechanism that we're trying to describe, not who would do it or how you would get it done.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's how you would know to trust that entity. How you as a certificate purchaser would know to trust a particular company that was selling certificates.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
So that is a question for the Policy Committee, establish a policy on how to know.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right, so what we're debating here is what are the words.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
We're debating here the answer to that question, it seems to me, to help the Policy Committee understand the question too.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, defining a mechanism for establishing, reliability was Joy's word, but it's not just reliability, because that's just—

John Moehrke – Interoperability & Security, GE – Principal Engineer
Within the Direct Project we did something similar, and I'm looking—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, actually, Arien, I think, is the person who brought this up, honestly.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I'm looking for what words we use there, because—

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Authenticity. It's legitimacy, authenticity.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Legitimacy and trustworthiness.

John Moehrke – Interoperability & Security, GE – Principal Engineer
How do you do that?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. I would say authenticity or legitimacy is the ... authenticity ....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And trustworthiness of defining a mechanism for establishing the legitimacy and trustworthiness of a certificate authority. Okay.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Does that take care of the third sub-bullet there?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I think it does.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
So what it says is we need policy around CAs and the certificates that they issue. The first sub-bullet is "Defining the level of assurance that must be achieved prior to issuing the digital certificates," and then in parentheses it says "identity proofing." The second one says, "Defining a mechanism for establishing the legitimacy and trustworthiness of a certificate authority."

John Moehrke – Interoperability & Security, GE – Principal Engineer
Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Business practices, okay. It's ten minutes to one and we probably aren't going to get to our next topic today. But—

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Let me just say a couple of words before we go to the public comment, Dixie, if that's okay, or what do you want to do?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I want to just thank everybody for dialing in today. I personally thought that this was a great discussion, so thank you all. Walter?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Indeed, thank you, yes. The only thing I want to say is that in the materials we included a copy of the recommendations on ELPDs. We will have a more detailed call devoted primarily to ELPDs. In fact, we have a two and a half hour call on Wednesday, March 16th and I know a few of you are not going to be able to be on that call, but I think what we will do then is basically focus on the entity level provider directory policy recommendations and then the areas where we need to define the requirements and the criteria for the standards for entity level provider directories.

You can browse and read through the recommendations that the Policy Committee approved on ELPDs from the slides, so I won't go through them in the slides here, but just generally there's two categories, two groups of actions that need to be taken regarding these recommendations on ELPDs. One is, actions related to the technical standards and what are the technical aspects of the standards to be used to have and create and operate at ELPDs. The other category of recommendations is really related to operational aspects of the ELPDs themselves. We don't need to get into those necessarily as the Privacy and Security Workgroup here, but those are the two categories of recommendations that you will see there, and again, we'll focus all our call on Wednesday of next week on to this. Maybe what we can do is jump to the slide on next steps, if that's okay, Dixie, with the slide that is going up on the screen right now.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's fine. I've got it back.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Right now we're showing on the screen the slide that talks about the work plan for the task through the end of March, and as you can see, we have March 16th devoted to the provider directory. The call will review the recommendations from the Policy Committee, we'll invite ONC to talk about how provider directories, entity level provider directories are being used in the Exchange and Direct Projects, and then we'll focus our attention on the requirements and the criteria for the standards. That will be the bulk of our call on the 16th. Then on March 24th, we'll use the March 24th call to probably finish up both the digital

certificate as well as the provider directory recommendations, finalize them before we present them to the full Standards Committee on the 28th.

Judy Sparrow – Office of the National Coordinator – Executive Director
Walter, that's the 29th, by the way.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Did I make a mistake? Okay, well is the 29th the meeting of the Standards Committee?

Judy Sparrow – Office of the National Coordinator – Executive Director
That's correct.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Oh, I'm sorry.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The 28th is a hearing, that's probably why it's on your—

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, I'm sorry. We'll fix that to the 29th, the full Health IT Standards Committee. So that's our schedule for the coming two, three weeks.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I feel comfortable that we'll at least have our recommendations for digital certificates and we will certainly have made good progress on the directories as well. I will update these slides with the changes we discussed today and I will talk to Mike Davis about the federal bridge arrangements before I send you the next version so that I'll have the information correct on these new slides about that—

John Moehrke – Interoperability & Security, GE – Principal Engineer
You can also check with Eric Kaplan, remember, he gave testimony on that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Eric ...?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Eric Kaplan was the one who gave testimony on—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Oh, I do remember, yes.

John Moehrke – Interoperability & Security, GE – Principal Engineer
He is the chair of the Security and Privacy Workgroup within the NHIN Exchange.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, he would be a good one to ask as well. Mike will know that as well, though, because he's involved in the whole NHIN Exchange with the VA and the DoD and Kaiser. But both of them would be good to check with. Okay. At any rate, once I get that information and feel like I have it ready for your review I'll send you the updated slides. But I think we're getting there and I really appreciate it. Any other comments before we go to public? Okay.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay, well thank you. Operator, can you see if anybody wishes to make a public comment?

Operator
We have no comments at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay, well thank you, Dixie, Walter, and everybody.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Thank you.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thanks, bye-bye.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Thanks, everyone. Bye-bye.

Public Comment Received During the Meeting

1. Doesn't a centralized CA result in issues related to a central unique identifier?

2. There will have to be a trusted escrow authority for every referential CA participant, and yet, no escrow contingencies are mentioned.

3. And what about the eventuality of deprecated (or horrors, defunct) CA repositories?

4. You don't put the private key in the message, but you use the private key to encode some part of the message?

5. Does this recommendation address any issues brought up in the PCAST Health IT Report?

6. i.e. certificates become universal identifiers which some might not like.

7. PKI should be spelled out when it first appears.